1/2

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/078,245 | 02/15/2002 | Samuli Mattila | 540-017-2 | 3221 |

4955 7590 10/05/2005

WARE FRESSOLA VAN DER SLUYS &
ADOLPHSON, LLP
BRADFORD GREEN BUILDING 5
755 MAIN STREET, P O BOX 224
MONROE, CT 06468

| EXAMINER | |
|---|---|
| LEMMA, SAMSON B | |
| **ART UNIT** | **PAPER NUMBER** |
| 2132 | |

DATE MAILED: 10/05/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/078,245 | MATTILA, SAMULI | |
| | Examiner | Art Unit | |
| | Samson B. Lemma | 2132 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *15 February 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *4 & 6*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.



AT

## *DETAILED ACTION*

1. **Claims 1-19** have been examined.

## *Priority*

2. Receipt is acknowledged of papers submitted under 35 U.S.C. 119 (a)-(d), which papers have been placed of record in the file.

## *Claim Rejections - 35 USC § 102*

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. **Claims 1-19** are rejected under 35 U.S.C. 102(e) as being anticipated by **Turnbull et al** (hereinafter referred as **Turnbull**) (Patent No. 6,092,201)(filed on Jan 27,1998)

5. **Claims 1-19** are also rejected under 35 U.S.C. 102(b) as being anticipated by **Bruce Schneier "Applied Cryptography" Second Edition 1996** (hereinafter referred as **Schneier**) (See reference U)

6. As per claim 1,8-9,10,14 **Turnbull discloses a method for providing authentication for setting up secure connections between a plurality of network nodes [Abstract, the first 4 lines, column 3, lines 14-19]** ( A method and apparatus for extending secure communication operations via shared lists is accomplished by creating a shared list in accordance with **authorization parameters** by one user and subsequently accessing the shared list via the authorization parameters by this and other users)**comprising at least the steps of placing a collection of accepted certificates comprising at least one accepted certificate available for other nodes by said first node [Abstract, the last 13 lines; column 3, lines 24-37] (Having identified another user, the user/first node** creating the **shared list which is a collection of accepted certificates** verifies that the secure communication parameters (which includes a public key certificate of an end-user or of a certification authority) it has received regarding another user is **trustworthy**. If the secure communication parameters are identified as **trustworthy/accepted certificate**, the secure communication parameters of **the another user are added to the shared list.** To authenticate the shared list, the user creating the list digitally signs it. **Once the shared list is created or once a collection of accepted certificate is created by the first node, other users**, if authorized, may access **the shared list** or **a collection of accepted certificate** to obtain certificates)

- **Importing said collection by at least one other node than said first node,** [Column 3, lines 35-41, column 6, lines 7-23] (As explained on column 35-37, once the

list is created, other users/nodes, could access the shared list to import/retrieve certificates)

- **Setting up of at least one secure connection by at least one of said at least one other node to a destination node whose certificate was imported as a part of said collection, and automatically accepting the authenticity of said destination node.**[column 6, lines 28-43 and figure 2] (As explained on column 3, lines 33-37, To authenticate the shared list/which includes destination node (i.e. allowing subsequent verification of its authenticity), the user creating the list signs it. Once the list is created, other users/other node, may access the shared list to retrieve certificates of the users contained in the list which includes the destination node. And as explained on column 3, lines 41-45, the other node can set secure communications, i.e., encrypt outgoing messages with the public keys of the intended recipients/destination node whose certificate has been retrieved/imported and verify signatures on received messages coming from the destination node then automatically accepting the authenticity of said destination node.)

7. **As per claim 2, 7,13,15 Turnbull discloses a method in a network node for setting up secure connections between the node and other network nodes [Abstract, the first 4 lines, column 3, lines 14-19]** ( A method and apparatus for extending secure communication operations via shared lists is accomplished by creating a shared list in accordance with **authorization parameters** by one user and subsequently accessing the shared list via the authorization parameters by this and other users) **comprising** at **least the steps of:**

- **Automatically obtaining a certificate of a second node by the network node.** [Column 5, lines 62-column 6, line 2] (As explained on column 5, lines 62-column 6, line 2, the end-user/network node 14 shown on figure 2 adds/obtains the

certificate of the second node which could be end-user 50 or end-user 62 shown on figure 2 automatically if the network node verifies the certification is trustworthy and network node 14 verify the trustworthiness of the certificates via personal contact or other methods)

- **Displaying at least an identification string of said certificate to the user of the network node, receiving an indication of acceptance or rejection of trust regarding said certificate from said** [Column 5, lines 62-column 6, line 2] (As explained on column 5, lines 62- column 6, line 2, the end-user/network node 14 shown on figure 2 adds the certificate of the second node which could be end-user 50 or end-user 62 shown on figure 2 automatically if the **network node verifies the certification is trustworthy** and network node 14 verify the trustworthiness of the **certificates via personal contact or other methods**, the network node 14 can **therefore accept or reject of the trust** regarding the certificate of **the 2nd end-user/network node depending on the verification test** the displaying of an identification string of said certification to the user of the network node is inherently included in the verification step since the network node 14 would not be able to verify the trustworthiness of the second node with out identification) and

- **In the case of receiving an indication of acceptance, storing at least an indication of the acceptance and said certificate, setting up a secure connection from the network node to said second node, and placing a collection of accepted certificates comprising at least one accepted certificate available for other nodes by the network node. [Column 6, lines 34-43 and column 5, lines 62- column 6, line 2, and column 6, lines 7-10; ] (As explained on column 5, lines 62-column 6, line 2,** End-user 14/network node 14 after accepting the trustworthiness of the second

node/other node, places/stores the second node in a shared list which includes a collection of accepted certificate this inherently includes an indication of acceptance including the certificate of the second node. As explained on the column 6, lines 34-43, secure communication from the network node to the second node is achieved. And as explained on column 6, lines 7-10, The list which is a collection of accepted certificates comprises at least one accepted certificate available/readily accessible to at least one end-user/other node who desires access to the security parameters of users in the functional grouping.)

8. **As per claim 3 Turnbull discloses a method/system/computer program as applied to claims above. Furthermore Turnbull discloses the method/system/computer program further comprising at least the step of digitally signing said collection by said first node.** (Abstract, lines 16-17'(To authenticate the shared list/collection by first node, the user creating the list digitally signs it.)

9. **As per claim 4 Turnbull discloses a method/system/computer program as applied to claims above. Furthermore Turnbull discloses the method/system/computer program further comprising at least the steps of encryption of said collection by said first node. [Abstract, lines 16-17]** (To authenticate the shared list/collection by first node, the user creating the list digitally signs it. Digital sings it means encrypting said the collection by the private key of the first node.)

10. **As per claim 5 Turnbull discloses a method/system/computer program as applied to claims above. Furthermore Turnbull discloses the method/system/computer program** further comprising at least the step of saving certificate use policy information in said collection by said first node.[claim 7] (Determining policy compliance of creation, modification, and usage of the shared list.)

11. **As per claim 6 Turnbull discloses a method/system/computer program as applied to claims above. Furthermore Turnbull discloses the method/system/computer program further comprising at least the step of digitally signing each certificate in said collection by said first node.** (Abstract, lines 16-17'(To authenticate the shared list/collection by first node, the user creating the list digitally signs it.)

12. **As per claims 11-12 Turnbull discloses a method/system/computer program as applied to claims above. Furthermore Turnbull discloses the method/system/computer program** further comprising firewall functionality and/ or an IPSec client program. [column 4, lines 1-2; claim 18]

13. **As per claims 16-19 Turnbull discloses a method/system/computer program as applied to claims above. Furthermore Turnbull discloses the method/system/computer program** further comprising the step of determining a **parameter value** based at least in part on information in said received certificate.[column 3, lines 26] ("secure communication **parameter** ")

14. **As per claims 1-19**, the core of the invention as disclosed by the applicant is explained on the abstract is to alleviate the problem of checking the identity of others by creating a mechanism, which allows users to trust and utilize the checking work performed by certain other users, so that every user need not check and confirm the identity of every other user. This can be accomplished by allowing a user who has checked that the identity of a number of other users truly correspond to their certificates, produce a list of these checked certificates, so that other users can import the list of checked certificates into their systems. "

(The limitation recited **in the claims 1-19** are based on the above principles and all are disclosed by **Schneier** on page 585, page 586, figure 24.7 and also on page 187, under the title "Distributed key Management ")

## *Conclusion*

15. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.(See PTO-Form 892).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA

S.L.

09/27/2005

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100